Cluster Security and Operations

Cluster security and operations.
This topic covers cluster security and management.
SSH is a utility for logging in to and
remotely executing commands on a remote server.
With Linux-based HDInsight, SSH establishes
an encrypted connection to the cluster head node and
provides a command line that you can use to type in commands.
Commands are then executed directly on the server.
SSH can be used to tunnel local requests
such as web requests to the HDInsight cluster.
The request will then be routed to the request resource
as if it had originated on the HDInsight cluster head node.
When creating a Linux-based HDInsight cluster,
you must provide the public key created previously.
From Windows-based clients,
there are two ways to create a Linux-based HDInsight cluster.
First the Azure Portal uses a web-based portal to
create the cluster.
And the Azure CLI for Mac, Linux, and
Windows, uses command line commands to create the cluster.
When using the Azure Portal to create a Linux-based HDInsight
cluster, you must enter an SSH username, and
select to either enter a password or SSH public key.
If you select SSH Public Key,
you can either paste the public key,
displayed in the Public Key for pasting into OpenSSH authorized
keys file field in PuttyGen into the SSH PublicKey field.
Or select, Select the file to browse and
select the file that contains the public key.
This creates a login for the specified user, and enables
either password authentication, or SSH key authentication.
Using the Azure Portal you can manage
Linux based clusters in Azure HD Insight.
Use the tab selector for information on creating
Hadoop clusters in HDInsight using other tools.
Settings and all settings displays the settings blade for
the cluster, which allows you to access detailed configuration
information for the cluster.
Dashboard, cluster dashboard, and URL.
These are all the ways to access the cluster dashboard
which is for Linux-based clusters.
Secure shell shows the instructions to connect
to the cluster using secure shell SSH connection.
Scale cluster allows you to change the number of worker
nodes for this cluster.
Delete deletes the cluster.
Quickstart displays information that will help you get started
using HDInsight.

Users allows you to set permission for portal management
for this cluster for other users on your Azure subscriptions.
Tags, tags allows you to set key value pairs
to define a custom taxonomy of your cloud services.
For example, you may create a key name project and
then use a common value for
all services associated with the specific project.
Ambari Views links to Ambari Web.
The Azure portal lets you view and
change the following settings.
Cluster log in change the cluster the HTTP username and
password, HDInsight partner add or
remove the current HDInsight partner.
External metastores via the Hive and oozie metastores.
The metastores can only be configured during the cluster
creation process.
Script actions, run bash scripts on the cluster.
Properties, to view the cluster properties.
Azure storage keys, view the default storage account, and
its key.
The storage account is configured during the cluster
creation process.
Cluster AAD Identity.
Users allows you to set permissions for
portal management of this cluster for
other users of your Azure subscription.
The resource usage of overview, shows the number of cores
consumed by this and other clusters, as well as the number
of cores available for additional clusters.
Using the Azure Portal,
you can reconfigure Linux based clusters in Azure HDN site.
Scale cluster allows to change the number of worker nodes for
this cluster.
The user setting allows you to set permissions for
portal management of this cluster for
other users on your Azure subscription.
Role-based access control are back enable access management
for Azure resources.
Using r-back you can segregate duties within your team and
grant only the amount of access to users, groups and
applications that they need to perform their jobs.
This table shows the roles and associated privileges used in
r-back for accessing Linux based clusters in Azure HDInsight.
The owner role allows access to all resources and actions within
an automation account including providing access to other users,
groups, and applications to manage the automation accounts.
The contributor role allows you to manage everything except
modifying other users access permissions to an automation
account.
The reader role allows you to view all the resources in

an automation account but cannot make any changes.
And the user access administrator role allows you to
manage user access to Azure automation accounts.
Deleting a cluster will not delete the default
storage account or any linked storage accounts.
You can recreate the cluster by using the same storage accounts
and the same metastores.
It is recommended that you use a new default blob container when
you recreate the cluster.
Auditing capabilities allow you to gain deeper insights on
the operations of your Azure resources and
consume this data in flexible ways.
The audit logs can be filtered based on a number
of parameters depending on the unique needs.